No-Failure Design
and
Disaster Recovery

Lessons from Fukushima

Yakov Ben-Haim

Technion

Israel Institute of Technology

lectures\talks\lib\no-fail-disas-rec01.tex 3.12.2014

Contents

1 *Highlights*

§ Major nuclear reactor accidents occur.

§

§ **Major nuclear reactor accidents occur.**

§ **Use models & data for analysis and design.**

§

§ **Major nuclear reactor accidents occur.**

§ **Use models & data for analysis and design.**

§ **Face severe requirements.**

E.g. Require very low probability of failure.

§

§ **Major nuclear reactor accidents occur.**

§ **Use models & data for analysis and design.**

§ **Face severe requirements.**

E.g. Require very low probability of failure.

§ **Questions:**

- **Can we optimize our designs?**
-

§ **Major nuclear reactor accidents occur.**

§ **Use models & data for analysis and design.**

§ **Face severe requirements.**

E.g. Require very low probability of failure.

§ **Questions:**

- **Can we optimize our designs?**
- **Can we reliably predict performance?**

§

§ **Major nuclear reactor accidents occur.**

§ **Use models & data for analysis and design.**

§ **Face severe requirements.**

E.g. Require very low probability of failure.

§ **Questions:**

- **Can we optimize our designs?**
- **Can we reliably predict performance?**

§ **Challenge: Uncertainty. Info-gaps.**

§

§ **Major nuclear reactor accidents occur.**

§ **Use models & data for analysis and design.**

§ **Face severe requirements.**

E.g. Require very low probability of failure.

§ **Questions:**

- **Can we optimize our designs?**
- **Can we reliably predict performance?**

§ **Challenge: Uncertainty. Info-gaps.**

§ **Innovation dilemma.**

§

§ **Major nuclear reactor accidents occur.**

§ **Use models & data for analysis and design.**

§ **Face severe requirements.**

E.g. Require very low probability of failure.

§ **Questions:**

- Can we optimize our designs?
- Can we reliably predict performance?

§ **Challenge: Uncertainty. Info-gaps.**

§ **Innovation dilemma.**

§ **No-fail design vs disaster recovery capability.**

2 Lessons of Fukushima: No-Failure Design and Disaster Recovery

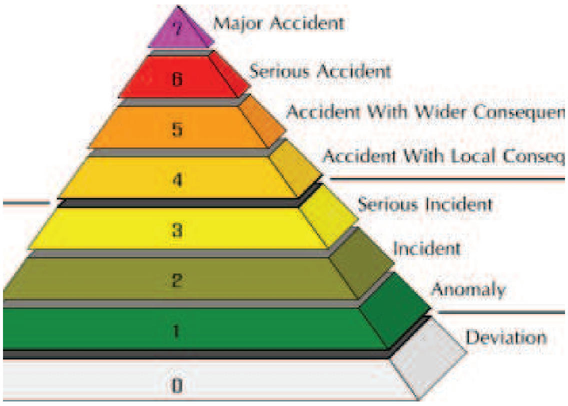


Figure 1: **Int'l Nuclear Event Scale.** (Wikipedia)

§ Nuclear plant accidents:

- **Major (INES 7):**
  - **Fukushima, Japan 11.3.2011.**
  - **Chernobyl, Ukraine, 26.4.1986.**
-

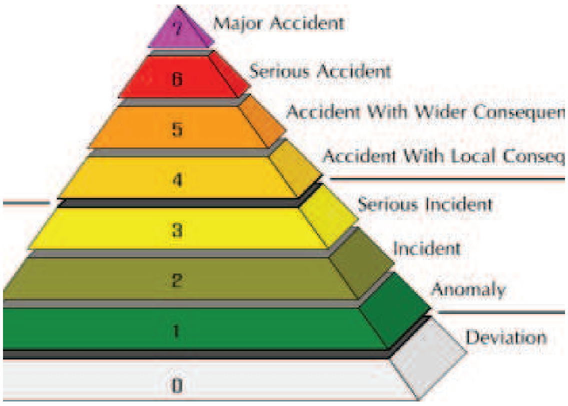


Figure 2: **Int'l Nuclear Event Scale.** (Wikipedia)

§ Nuclear plant accidents:

- **Major (INES 7):**
  - **Fukushima, Japan 11.3.2011.**
  - **Chernobyl, Ukraine, 26.4.1986.**
- **Serious (INES 6):**
  - **Kyshtym, USSR, 29.9.1957.**
-

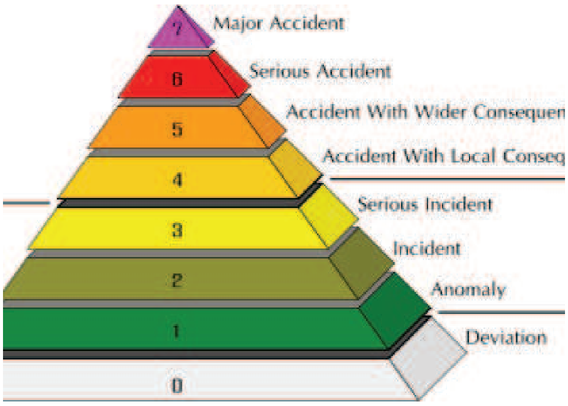


Figure 3: **Int'l Nuclear Event Scale.** (Wikipedia)

§ Nuclear plant accidents:

- **Major (INES 7):**
  - **Fukushima, Japan 11.3.2011.**
  - **Chernobyl, Ukraine, 26.4.1986.**
- **Serious (INES 6):**
  - **Kyshtym, USSR, 29.9.1957.**
- **With wider consequences (INES 5):**
  - **Windscale fire, UK, 10.10.1957**
  - **3 Mile Island, Harrisburg, PA, 28.3.1979.**
  - **Lucens partial core meltdown (Switzerland), 21.1.1969**
  - **Others.**

§ Approx nuclear power statistics (Aug 2011):

- **432 reactors in 30 countries (ENS).**[‡]
- **366GWe installed capacity (ENS).**
- **14,570 reactor years of experience (ENS).**
-

[‡] European Nuclear Society http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm

§ Approx nuclear power statistics (Aug 2011):

- **432 reactors in 30 countries (ENS).**[‡]
- **366GWe installed capacity (ENS).**
- **14,570 reactor years of experience (ENS).**
- **1 major accident in industrial democracy.**
-

[‡] European Nuclear Society http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm

§ Approx nuclear power statistics (Aug 2011):

- **432 reactors in 30 countries (ENS).**[‡]
- **366GWe installed capacity (ENS).**
- **14,570 reactor years of experience (ENS).**
- **1 major accident in industrial democracy.**
- $\frac{1}{14,570} = 6.8635 \times 10^{-5}$ **major acc/rtr yr.**[†]
-

[‡] European Nuclear Society http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm

[†] This is probably a substantial under-estimate. The numerator is too small: 3 reactors were seriously damaged, not 1. The denominator is too large: we should only take reactor-years from industrial democracies.

§ Approx nuclear power statistics (Aug 2011):

- **432 reactors in 30 countries (ENS).**[‡]
- **366GWe installed capacity (ENS).**
- **14,570 reactor years of experience (ENS).**
- **1 major accident in industrial democracy.**
- $\frac{1}{14,570} = 6.8635 \times 10^{-5}$ **major acc/rtr yr.**
- $\left(1 - 6.8635 \times 10^{-5}\right)^{432} = \mathbf{0.97}$

= prob. of no major accident in 1 calendar year.

-

‡ European Nuclear Society http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm

§ **Approx nuclear power statistics (Aug 2011):**

- **432 reactors in 30 countries (ENS).**[‡]
- **366GWe installed capacity (ENS).**
- **14,570 reactor years of experience (ENS).**
- **1 major accident in industrial democracy.**
- $\frac{1}{14,570} = 6.8635 \times 10^{-5}$ **major acc/rtr yr.**
- $\left(1 - 6.8635 \times 10^{-5}\right)^{432} = \mathbf{0.97}$

  $=$ **prob. of no major accident in 1 calendar year.**
- $1 - 0.97 = \mathbf{0.03}$

  $=$ **3% prob. of major accident in 1 calendar year**

  $=$ **33 year recurrence time for INES 7.**

§

[‡] European Nuclear Society http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm

§ **Approx nuclear power statistics (Aug 2011):**

- **432 reactors in 30 countries (ENS).**[‡]
- **366GWe installed capacity (ENS).**
- **14,570 reactor years of experience (ENS).**
- **1 major accident in industrial democracy.**
- $\frac{1}{14,570} = 6.8635 \times 10^{-5}$ **major acc/rtr yr.**
- $\left(1 - 6.8635 \times 10^{-5}\right)^{432} = \mathbf{0.97}$

  = **prob. of no major accident in 1 calendar year.**
- $1 - 0.97 = \mathbf{0.03}$

  = **3% prob. of major accident in 1 calendar year**

  = **33 year recurrence time for INES 7.**

§ **This is probably optimistic. Ignoring:**

- **3 core-damaged rtr's at Fukushima.**
- **Including all rtr yrs, not industrial democracy.**
- **Ignoring INES 6, 5, 4 accidents.**

§

[‡] European Nuclear Society http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm

§ **Approx nuclear power statistics (Aug 2011):**

- **432 reactors in 30 countries (ENS).**[‡]
- **366GWe installed capacity (ENS).**
- **14,570 reactor years of experience (ENS).**
- **1 major accident in industrial democracy.**
- $\frac{1}{14,570} = 6.8635 \times 10^{-5}$ **major acc/rtr yr.**
- $\left(1 - 6.8635 \times 10^{-5}\right)^{432} = \mathbf{0.97}$

  = **prob. of no major accident in 1 calendar year.**
- $1 - 0.97 = \mathbf{0.03}$

  = **3% prob. of major accident in 1 calendar year**

  = **33 year recurrence time for INES 7.**

§ **This is probably optimistic. Ignoring:**

- **3 core-damaged rtr's at Fukushima.**
- **Including all rtr yrs, not industrial democracy.**
- **Ignoring INES 6, 5, 4 accidents.**

§ **Is 33 year recurrence long or short?**

[‡] European Nuclear Society http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm

§ Lessons:

- **Design for No-Failure. (Failures are serious.)**
-

§ Lessons:

- **Design for No-Failure. (Failures are serious.)**
- **Prepare Disaster Recovery Capability. (They occur.)**

§

§ Lessons:

- **Design for No-Failure. (Failures are serious.)**
- **Prepare Disaster Recovery Capability. (They occur.)**

§ Challenges:

- **Why do we need DRC if we do No-Fail Design?**
    -

§ Lessons:

- Design for No-Failure. (Failures are serious.)
- Prepare Disaster Recovery Capability. (They occur.)

§ Challenges:

- Why do we need DRC if we do No-Fail Design?
  - Resource allocation.
  -

§ Lessons:

- Design for No-Failure. (Failures are serious.)
- Prepare Disaster Recovery Capability. (They occur.)

§ Challenges:

- Why do we need DRC if we do No-Fail Design?
  - Resource allocation.
  - Public relations.
-

§ Lessons:

- Design for No-Failure. (Failures are serious.)
- Prepare Disaster Recovery Capability. (They occur.)

§ Challenges:

- Why do we need DRC if we do No-Fail Design?
  - Resource allocation.
  - Public relations.
- Moral hazard paradox:
  - No-Fail & DRC teams: must be independent.
  -

§ Lessons:

- Design for No-Failure. (Failures are serious.)
- Prepare Disaster Recovery Capability. (They occur.)

§ Challenges:

- Why do we need DRC if we do No-Fail Design?
  - Resource allocation.
  - Public relations.
- Moral hazard paradox:
  - No-Fail & DRC teams: must be independent.
  - No-Fail & DRC teams: must cooperate.
-

§ Lessons:

- Design for No-Failure. (Failures are serious.)
- Prepare Disaster Recovery Capability. (They occur.)

§ Challenges:

- Why do we need DRC if we do No-Fail Design?
  - Resource allocation.
  - Public relations.
- Moral hazard paradox:
  - No-Fail & DRC teams: must be independent.
  - No-Fail & DRC teams: must cooperate.
- Uncertainty:
  - Can we reliably predict performance?
  -

§ Lessons:

- Design for No-Failure. (Failures are serious.)
- Prepare Disaster Recovery Capability. (They occur.)

§ Challenges:

- Why do we need DRC if we do No-Fail Design?
  - Resource allocation.
  - Public relations.
- Moral hazard paradox:
  - No-Fail & DRC teams: must be independent.
  - No-Fail & DRC teams: must cooperate.
- Uncertainty:
  - Can we reliably predict performance?
  - Can we optimize our designs?

§

§ Lessons:

- Design for No-Failure. (Failures are serious.)
- Prepare Disaster Recovery Capability. (They occur.)

§ Challenges:

- Why do we need DRC if we do No-Fail Design?
  - Resource allocation.
  - Public relations.
- Moral hazard paradox:
  - No-Fail & DRC teams: must be independent.
  - No-Fail & DRC teams: must cooperate.
- Uncertainty:
  - Can we reliably predict performance?
  - Can we optimize our designs?

§ Are there more lessons or challenges from Fukushima?

3 *Science-Based Modeling*

§ Quantitative science-based models:

- **Used in design and strategic planning.**
-

§ Quantitative science-based models:

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**

§

§ **Quantitative science-based models:**

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**

§ **This is a modern utilitarian attitude to knowledge.**

§

§ **Quantitative science-based models:**

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**

§ **This is a modern utilitarian attitude to knowledge.**

§ **Traditional attitudes to knowledge:**

- **Socrates:**

  Artisans not wise. Practical knowledge is not wisdom.
  (*Apology*, 22d-e)
-

§ **Quantitative science-based models:**

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**

§ **This is a modern utilitarian attitude to knowledge.**

§ **Traditional attitudes to knowledge:**

- **Socrates:**
  Artisans not wise. Practical knowledge is not wisdom. (*Apology*, 22d-e)
- **Euclid: Gives student a coin so lesson worthwhile.**
-

§ Quantitative science-based models:

- Used in design and strategic planning.
- Enable responsible, reliable decisions.

§ This is a modern utilitarian attitude to knowledge.

§ Traditional attitudes to knowledge:

- **Socrates:**
  Artisans not wise. Practical knowledge is not wisdom. (*Apology*, 22d-e)
- **Euclid:** Gives student a coin so lesson worthwhile.
- **Avika:** Don't live in a town whose mayor is a scholar. (*Pesahim*, ch. 10)
-

§ **Quantitative science-based models:**

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**

§ **This is a modern utilitarian attitude to knowledge.**

§ **Traditional attitudes to knowledge:**

- **Socrates:**

  Artisans not wise. Practical knowledge is not wisdom. (*Apology*, 22d-e)
- **Euclid: Gives student a coin so lesson worthwhile.**
- **Avika: Don't live in a town whose mayor is a scholar. (*Pesahim*, ch. 10)**
- **Rambam argues that science leads to love of God. (*Mishneh Torah*, bk. 1)**

§

§ **Quantitative science-based models:**

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**

§ **This is a modern utilitarian attitude to knowledge.**

§ **Traditional attitudes to knowledge:**

- **Socrates:**

  Artisans not wise. Practical knowledge is not wisdom. (*Apology*, 22d-e)
- **Euclid: Gives student a coin so lesson worthwhile.**
- **Avika: Don't live in a town whose mayor is a scholar. (*Pesahim*, ch. 10)**
- **Rambam argues that science leads to love of God. (*Mishneh Torah*, bk. 1)**

§ **We must understand the modern attitude: strengths and limitations.**

Fundamental Physics

Maxwell's Equations

Figure 4: **James Clerk Maxwell, 1831–1879.**

$$\nabla \cdot E = \frac{\rho}{\varepsilon} \qquad \nabla \cdot B = 0$$

$$\nabla \times E = -\frac{\partial B}{\partial t} \qquad \nabla \times B = \mu J + \mu\varepsilon\frac{\partial E}{\partial t}$$

- **Positivism: From basic science to technology:**
  Radio, X-ray diagnosis, CAT scan,
  wifi, remote sensing, ...

- **Engineering education: sciences not crafts.**

Empirical Physics

Finite Element Modeling

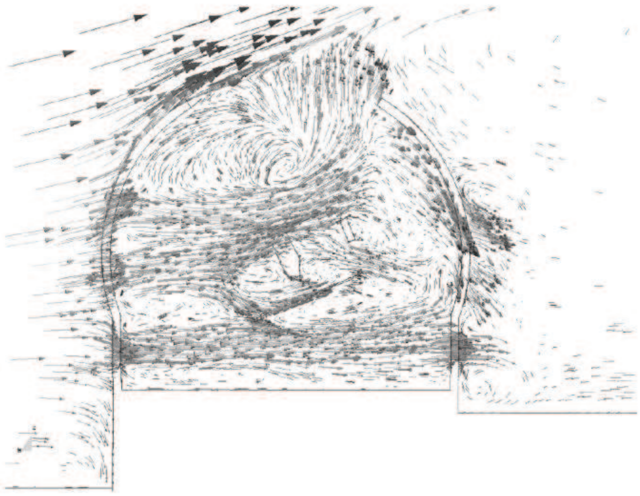


Figure 7: Example of velocity field on the vertical mid section

Figure 5: **Velocity field around a structure.**‡

- **If we know the physics**

  we can

  calculate anything.

- **Methodology: simulation vs experiment.**

‡R. Codina, C. Morton, E. Oñate and O. Soto, http://www.cimne.com/eo/publicaciones/files/PI181.pdf

Computational Social Science

Econometric Modeling


$$\frac{\mathrm{d}u(c_t)}{\mathrm{d}c_t}p_{1t} = \beta\frac{\mathrm{d}u(c_{t+1})}{\mathrm{d}c_{t+1}}(1-\widehat{\alpha}\phi_t)\widetilde{y}_{1,t+1}$$
$$\frac{\mathrm{d}u(c_t)}{\mathrm{d}c_t}p_{2t} = \beta\frac{\mathrm{d}u(c_{t+1})}{\mathrm{d}c_{t+1}}y_{2,t+1}$$

Figure 6: **$100, US GDP growth,[‡] Lucas asset pricing model.**

- **From the dry science**

  to

  policy formulation.

- **Methodology: social engineering.**

\lectures\talks\lib\modeling-econ01.tex 27.11.2013

[‡] Saul H. Hymans, Forecasting and Econometric Models, The Concise Encyclopedia of Economics, http://www.econlib.org/library/Enc/ForecastingandEconometricModels.html

Computational Megalomania?

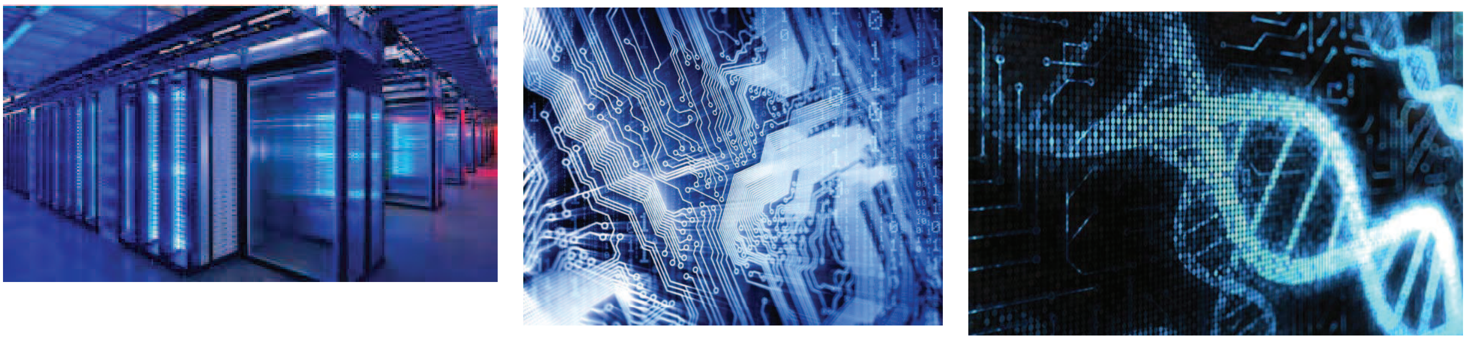


Figure 7: **Computers and their aspirations.**

- **If you can't measure it, it's not real (logical positivism).**
-

Computational Megalomania?

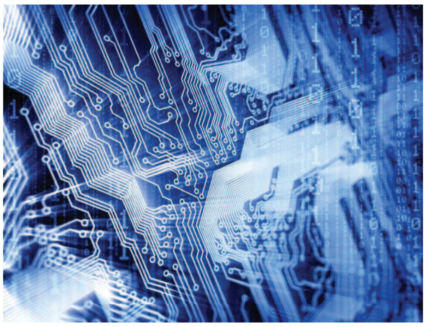




Figure 8: **Computers and their aspirations.**

- **If you can't measure it, it's not real (logical positivism).**
- **If it's not a number, it's not important.**
  (What about meaning?)
-

Computational Megalomania?

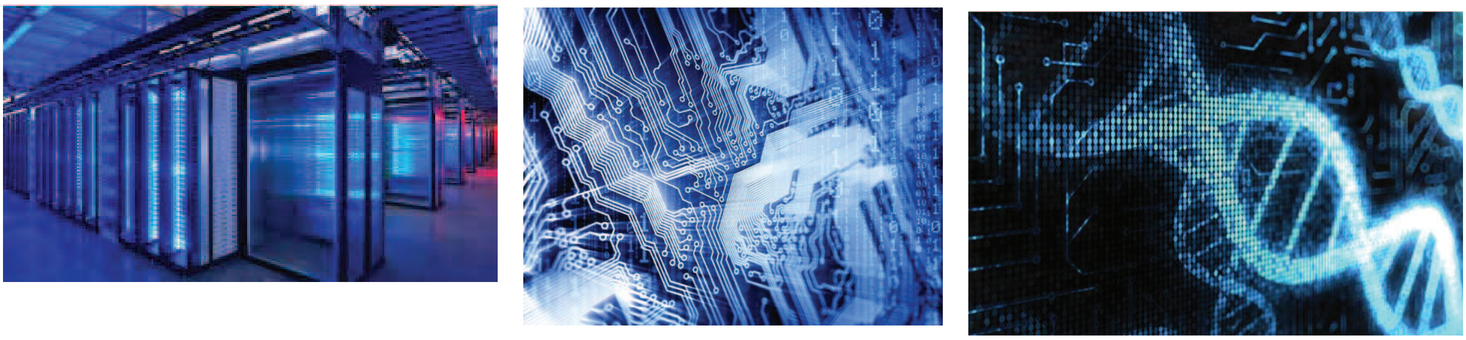


Figure 9: **Computers and their aspirations.**

- **If you can't measure it, it's not real (logical positivism).**
- **If it's not a number, it's not important. (What about meaning?)**
- **We can compute anything. (Archimedes' modern lever?)**

∼∼*Modeling: Conclusion*∼∼

§ Quantitative model types:

- **Fundamental physics.**
- **Empirical physics.**
- **Computational social science.**
- **Computational megalomania?**

§

~~*Modeling: Conclusion*~~

§ Quantitative model types:

- Fundamental physics.
- Empirical physics.
- Computational social science.
- Computational megalomania?

§ Quantitative model uses:

- Used in design and strategic planning.
-

∼∼*Modeling: Conclusion*∼∼

§ Quantitative model types:

- **Fundamental physics.**
- **Empirical physics.**
- **Computational social science.**
- **Computational megalomania?**

§ Quantitative model uses:

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**
-

∼∼Modeling: Conclusion∼∼

§ Quantitative model types:

- Fundamental physics.
- Empirical physics.
- Computational social science.
- Computational megalomania?

§ Quantitative model uses:

- Used in design and strategic planning.
- Enable responsible, reliable decisions.
- Modern utilitarian attitude to knowledge.

§

∼∼Modeling: Conclusion∼∼

§ Quantitative model types:

- **Fundamental physics.**
- **Empirical physics.**
- **Computational social science.**
- **Computational megalomania?**

§ Quantitative model uses:

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**
- **Modern utilitarian attitude to knowledge.**

§ The questions:

- **Can we reliably predict performance?**
-

∼∼*Modeling: Conclusion*∼∼

§ **Quantitative model types:**

- **Fundamental physics.**
- **Empirical physics.**
- **Computational social science.**
- **Computational megalomania?**

§ **Quantitative model uses:**

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**
- **Modern utilitarian attitude to knowledge.**

§ **The questions:**

- **Can we reliably predict performance?**
- **Can we realistically optimize the outcome?**

§

∼∼*Modeling: Conclusion*∼∼

§ **Quantitative model types:**

- **Fundamental physics.**
- **Empirical physics.**
- **Computational social science.**
- **Computational megalomania?**

§ **Quantitative model uses:**

- **Used in design and strategic planning.**
- **Enable responsible, reliable decisions.**
- **Modern utilitarian attitude to knowledge.**

§ **The questions:**

- **Can we reliably predict performance?**
- **Can we realistically optimize the outcome?**

§ **The challenge:**

Uncertainty, surprise, ignorance, change.

Info-gaps.

4 Info-Gap Uncertainty: Examples

\lectures\talks\lib\ig-unc01intro.tex 4.1.2011

∼∼*Thames Flood Barrier*∼∼

Figure 10: **1953 barrier breach.**

Figure 11: **Barrier element.**

§ Some facts:

- **1953: worst storm surge of century.**
- **Flood defences breached.**
- **307 dead. Thousands evacuated.**
- **Canvey Island in Estuary devastated.**
- **Current barrier opened May 1984.**

§ **Thames 2100:**

Major re-design of flood defences.

§ **Uncertainties:**

- **Statistics of surge height:**
  - **Fairly complete: most years since 1819.**
  - **Planning for 1000-year surge.**
- **Global warming: sea level rise.**
- **Tectonic settling of s. England.**
- **Damage vs flood depth.**
- **Human action: dredging, embanking.**
- **Urban development.**

§ **Severe Knightian uncertainties: Gaps in knowledge, understanding and goals.**

∼∼*Fukushima Nuclear Reactor*∼∼

Figure 12: **Sea wall breach.**

Figure 13: **Hydrogen explosion.**

§ Some facts:

- **11.3.2011: Richter-9 earthquake in NE Japan.**
- **Tsunami followed shortly.**
- **Sea wall breached: fig. 12.**‡
- **Hydrogen explosion several days later. Fig. 13.**‡
- **Slow disaster recovery.**

§ Info-gaps:

- **Sub-system interactions.**
- **Institutional constraints.**

‡ http://www.dailymail.co.uk/news/article-1388629/Japan-tsunami-destroyed-wall-designed-protect-Fukushima-nuclear-plant.html

∼∼*Assay Spatially Random Material*∼∼

Figure 14: **Nuclear Waste.**

Figure 15: **Gold Ore Vein.**

- **Detector type, location, number?**
- **Info-gaps:**
  - **Spatial distribution of analyte.**
  - **Spatial heterogeneity of matrix.**

∼∼Interest rate after 9/11∼∼

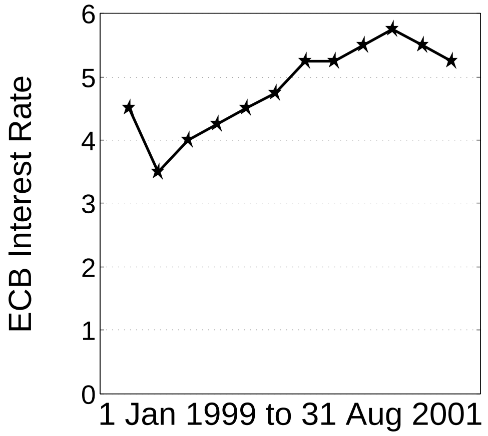


Figure 16: **ECB Interest Rates**

- **Rate fairly constant through Aug 2001**

∼∼*Interest rate after 9/11*∼∼

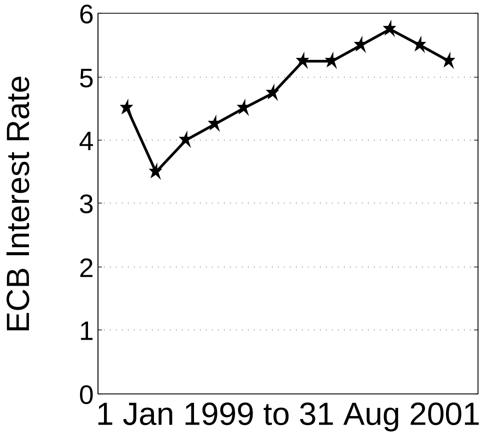


Figure 17: **ECB Interest Rates**

Figure 18: **11 Sept 2001.**

- **Rate fairly constant through Aug 2001**
- **After 9/11 ECB will reduce the rate.**
- **Info-gap:**
  - **Reduce by how much?**
  - **What is ECB decision model?**

∼∼*Climate Change*∼∼

§ The issue:

Sustained rise in green house gases

results in temperature rise

which results in adverse economic impact.

§ Models:

- Temperature change: $\Delta \mathrm{CO}_2 \Longrightarrow \Delta T$.
- Economic impact: $\Delta T \Longrightarrow \Delta \mathrm{GDP}$.

§ The problems:

- Models highly uncertain.
- Data controversial.

§ E.g., IPCC model for

Uncertainty in Equil'm Clim. Sensi'ty, S.

- **Likely range: 1.5$^{\mathrm{o}}$C to 4.5$^{\mathrm{o}}$C.**
- **Extreme values highly uncertain.**
- **95th quantile of S in 10 studies:**

  Mean: 7.1$^{\mathrm{o}}$C. St. Dev: 2.8$^{\mathrm{o}}$C.

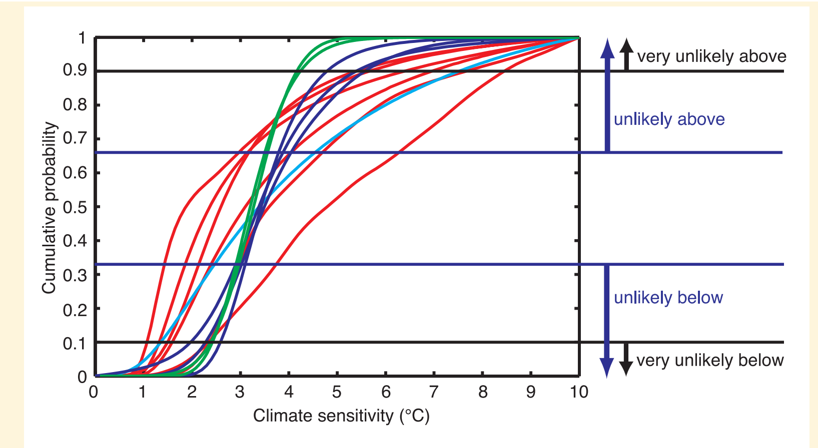


Figure 19: IPCC ch.10, p.799.

∼∼*Profiling Criminals*∼∼

Figure 20: **Profiling raises arrests.**

- **Profiling: focus policing resources.**
  - **Arrests rise in profiled group.**
  - **Crime rises in other groups.**
  - **Everybody happy?**
- **Info-gaps: Uncertain response functions.**

∼∼*Summary*∼∼

§ **Severe Knightian uncertainties: Gaps in knowledge, understanding and goals.**

§

∼∼*Summary*∼∼

§ **Severe Knightian uncertainties:** **Gaps in knowledge, understanding and goals.**

§ **Info-Gap models of uncertainty:**

- **Disparity between what is known and what needs to be known for responsible decision.**
-

∼∼*Summary*∼∼

§ **Severe Knightian uncertainties:** Gaps in **knowledge, understanding** and **goals.**

§ **Info-Gap models of uncertainty:**

- **Disparity between what is known and what needs to be known for responsible decision.**
- **Unbounded family of sets of events (points, functions or sets).**
- **No known worst case.**
- **No funcs. of probability, plausibility, likelihood, etc.**
- **Hybrid: info-gap model of probabilities.**

5 *Innovation Dilemma*

\lectures\talks\lib\innov-dilem01trunc.tex 7.5.2013

§ Choose between two options:

- **Option 1:**
  - **Innovative, promising, new technology.**
  - **Higher uncertainty because it's new.**
-

§ **Choose between two options:**

- **Option 1:**
  - **Innovative, promising, new technology.**
  - **Higher uncertainty because it's new.**
- **Option 2:**
  - **Standard. State of the art.**
  - **Lower uncertainty because it's well known.**

§ Examples of the innovation dilemma:

- **Automotive collision control:**
  - **Sensor-based computer control (innov).**
  - **Reliable effective breaking system (SotA).**
-

§ Examples of the innovation dilemma:

- **Automotive collision control:**
  - Sensor-based computer control (innov).
  - Reliable effective breaking system (SotA).
- **Eradicate invasive species:**
  - New aerial pesticide (innov).
  - Port quarantine (SotA).
-

§ Examples of the innovation dilemma:

- **Automotive collision control:**
  - Sensor-based computer control (innov).
  - Reliable effective breaking system (SotA).
- **Eradicate invasive species:**
  - New aerial pesticide (innov).
  - Port quarantine (SotA).
- **Nurture economic growth in 3rd world:**
  - Human capital, institutions (innov).
  - Import technology, infrastructure (SotA).
-

§ Examples of the innovation dilemma:

- **Automotive collision control:**
  - Sensor-based computer control (innov).
  - Reliable effective breaking system (SotA).
- **Eradicate invasive species:**
  - New aerial pesticide (innov).
  - Port quarantine (SotA).
- **Nurture economic growth in 3rd world:**
  - Human capital, institutions (innov).
  - Import technology, infrastructure (SotA).
- **Financial investment:**
  - New start-up firm (innov).
  - US Treasury bonds (SotA).
-

§ Examples of the innovation dilemma:

- **Automotive collision control:**
  - Sensor-based computer control (innov).
  - Reliable effective breaking system (SotA).
- **Eradicate invasive species:**
  - New aerial pesticide (innov).
  - Port quarantine (SotA).
- **Nurture economic growth in 3rd world:**
  - Human capital, institutions (innov).
  - Import technology, infrastructure (SotA).
- **Financial investment:**
  - New start-up firm (innov).
  - US Treasury bonds (SotA).
- **Risk taking or avoiding:**
  - Nothing ventured, nothing gained (innov).
  - Nothing ventured, nothing lost (SotA).

§ Decision strategies.

- **Outcome optimization:**
  - **Use models to predict outcomes.**
  - **Choose predicted best option.**
-

§ Decision strategies.

- **Outcome optimization:**
  - Use models to predict outcomes.
  - Choose predicted best option.
- **Max-min** (maximize the min reward):
  - Specify level of uncertainty.
  - Use models to predict worst outcomes.
  - Choose the best worst-outcome.
-

§ Decision strategies.

- **Outcome optimization:**
  - Use models to predict outcomes.
  - Choose predicted best option.
- **Max-min** (maximize the min reward):
  - Specify level of uncertainty.
  - Use models to predict worst outcomes.
  - Choose the best worst-outcome.
- **Robust satisficing:**
  - Specify critical outcome requirements.
  - Use models to predict robustness.
  - Choose best rbs of adequate outcome.
-

§ Decision strategies.

- **Outcome optimization:**
  - Use models to predict outcomes.
  - Choose predicted best option.
- **Max-min** (maximize the min reward):
  - Specify level of uncertainty.
  - Use models to predict worst outcomes.
  - Choose the best worst-outcome.
- **Robust satisficing:**
  - Specify critical outcome requirements.
  - Use models to predict robustness.
  - Choose best rbs of adequate outcome.
- **Opportune windfalling:**
  - Specify wonderful outcome aspiration.
  - Use models to predict opportuneness.
  - Choose best ops of wonderful outcome.

§

§ Decision strategies.

- **Outcome optimization:**
  - Use models to predict outcomes.
  - Choose predicted best option.
- **Max-min** (maximize the min reward):
  - Specify level of uncertainty.
  - Use models to predict worst outcomes.
  - Choose the best worst-outcome.
- **Robust satisficing:**
  - Specify critical outcome requirements.
  - Use models to predict robustness.
  - Choose best rbs of adequate outcome.
- **Opportune windfalling:**
  - Specify wonderful outcome aspiration.
  - Use models to predict opportuneness.
  - Choose best ops of wonderful outcome.

§ Question:

Which strategy suitable for innovation dilemma?

6 *Thames Flood Barrier*

Figure 21: **1953 barrier breach.**

Figure 22: **Barrier element.**

§ Some facts:

- **1953: worst storm surge of century.**
- **Flood defences breached.**
- **307 dead. Thousands evacuated.**
- **Canvey Island in Estuary devastated.**
- **Current barrier opened May 1984.**

§ Thames 2100:

Major re-design of flood defences.

§ Uncertainties:

- Statistics of surge height:
  - Fairly complete: most years since 1819.
  - Planning for 1000-year surge.
- Damage vs flood depth.
- Global warming: sea level rise.
- Human action: dredging, embanking.
- Urban development.
- Tectonic settling of s. England.

§ **Design requirement:**

Small probability of large damage.

§ **Decision:** **choose a design.**

§

§ **Design requirement:**

Small probability of large damage.

§ **Decision:** **choose a design.**

§ **Challenge: Uncertainty.**

- **Our data, understanding is limited.**
- **Our goals may be unclear, conflicting.**

§

§ **Design requirement:**

Small probability of large damage.

§ **Decision:** **choose a design.**

§ **Challenge: Uncertainty.**

- **Our data, understanding is limited.**
- **Our goals may be unclear, conflicting.**

§ **Design strategy: Robust satisficing.**

- **How wrong can we be, and the design is still adequate? (Satisficing.)**
- **How large a surprise can the design tolerate? (Robustness.)**

§ Innovation dilemma.

- **Design 1:**
  - **Innovative technology.**
    - — **Early warning system.**
    - — **Adaptive channeling.**
  -

§ Innovation dilemma.

- **Design 1:**
  - **Innovative technology.**
    - — **Early warning system.**
    - — **Adaptive channeling.**
  - **Predicted prob of excess damage: tiny.**
  - ○

§ Innovation dilemma.

- **Design 1:**
  - **Innovative technology.**
    - — **Early warning system.**
    - — **Adaptive channeling.**
  - **Predicted prob of excess damage: tiny.**
  - **Uncertainty: moderate.**
-

§ Innovation dilemma.

- **Design 1:**
  - **Innovative technology.**
    - — **Early warning system.**
    - — **Adaptive channeling.**
  - **Predicted prob of excess damage: tiny.**
  - **Uncertainty: moderate.**
- **Design 2:**
  - **State of the art technology.**
    - — **Solid dykes.**
    - — **Hydraulic barriers.**
  -

§ Innovation dilemma.

- **Design 1:**
  - **Innovative technology.**
    - — **Early warning system.**
    - — **Adaptive channeling.**
  - **Predicted prob of excess damage: tiny.**
  - **Uncertainty: moderate.**
- **Design 2:**
  - **State of the art technology.**
    - — **Solid dykes.**
    - — **Hydraulic barriers.**
  - **Predicted prob of excess damage: small.**
  -

§ Innovation dilemma.

- **Design 1:**
  - **Innovative technology.**
    - — **Early warning system.**
    - — **Adaptive channeling.**
  - **Predicted prob of excess damage: tiny.**
  - **Uncertainty: moderate.**
- **Design 2:**
  - **State of the art technology.**
    - — **Solid dykes.**
    - — **Hydraulic barriers.**
  - **Predicted prob of excess damage: small.**
  - **Uncertainty: tiny.**

§

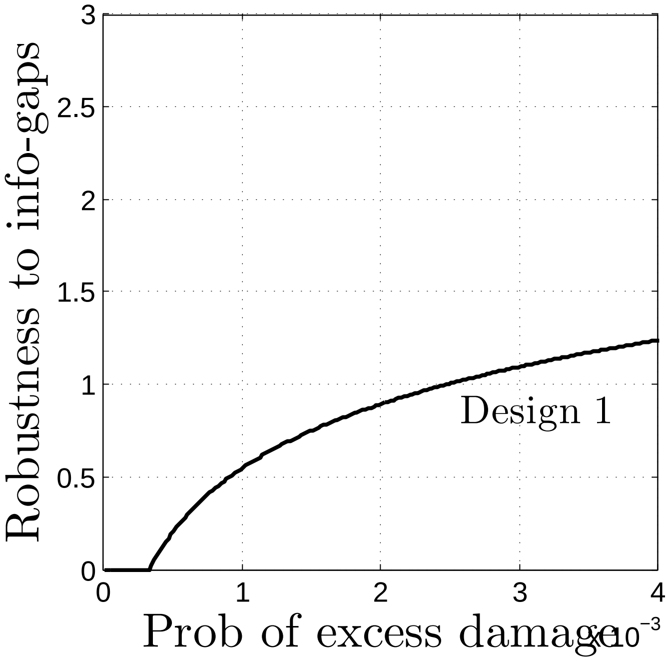
§ Innovation dilemma.

- **Design 1:**
  - **Innovative technology.**
    - — **Early warning system.**
    - — **Adaptive channeling.**
  - **Predicted prob of excess damage: tiny.**
  - **Uncertainty: moderate.**
- **Design 2:**
  - **State of the art technology.**
    - — **Solid dykes.**
    - — **Hydraulic barriers.**
  - **Predicted prob of excess damage: small.**
  - **Uncertainty: tiny.**

§ Choose design 1? Design 2?

- **Responsible decision?**
- **Robust to ignorance?**

§ Robustness to info-gaps vs Probability of excess damage. Design 1

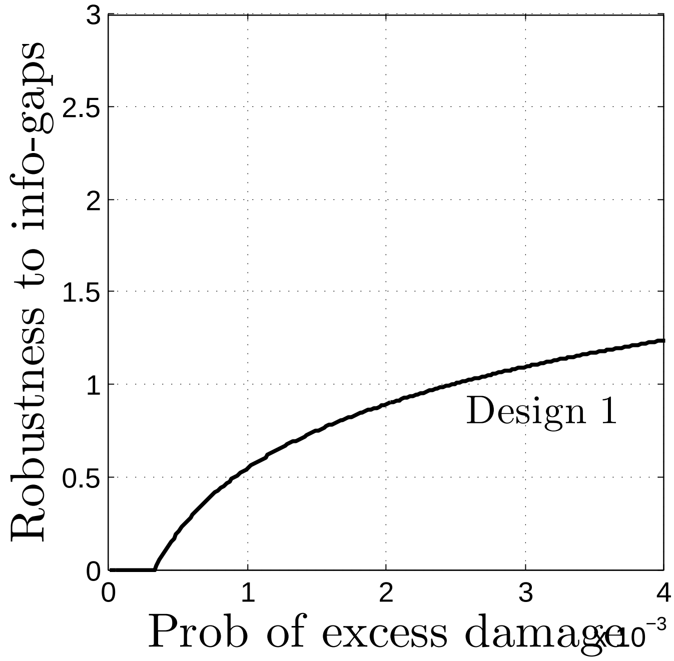


§ Trade off:

Less demanding outcome has greater robustness.

§

§ Robustness to info-gaps vs Probability of excess damage. Design 1



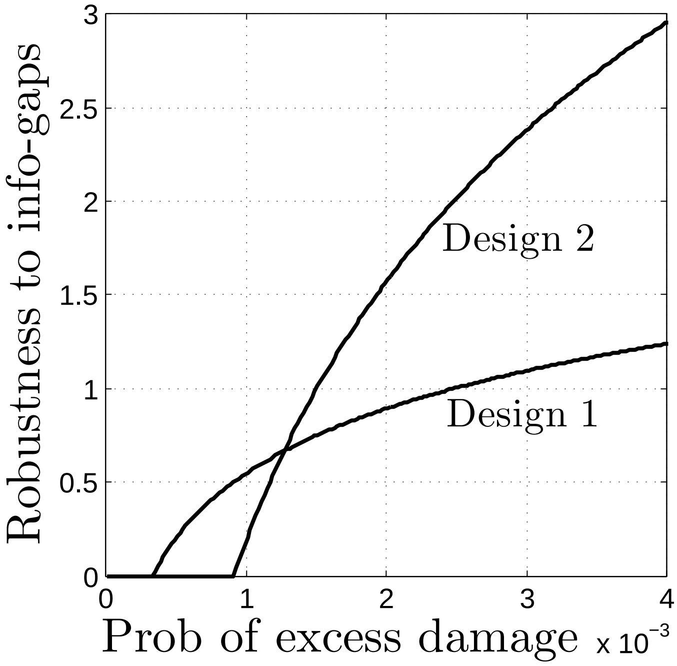
§ Trade off:

Less demanding outcome has greater robustness.

§ Zeroing:

Estimated outcome has zero robustness.

§ Comparing 2 designs.

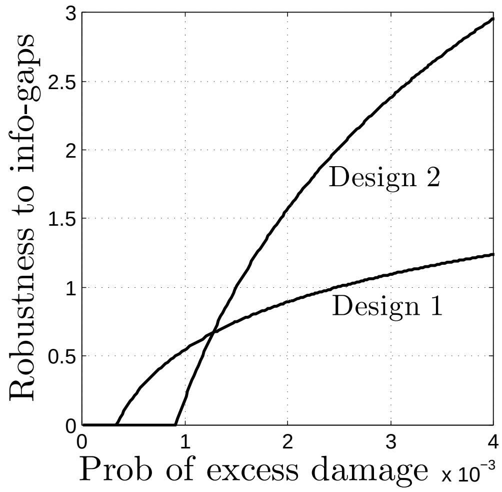


§ **Design 1 (innov) estimated to be better.**
Zero robustness of estimates.

§ **Design 2 (SotA) more robust for** $P > P_{\times}$.

§ **Innovation dilemma.**

§ Optimize or robust-satisfice?

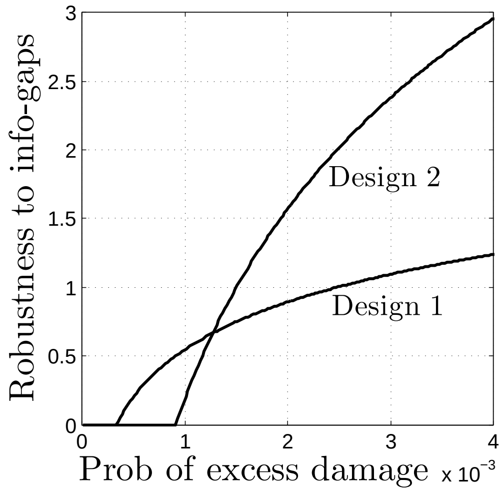


§ Outcome optimization:

- **Find best models. (Maybe probability.)**
- **Predict best-outcome design.**

§

§ Optimize or robust-satisfice?



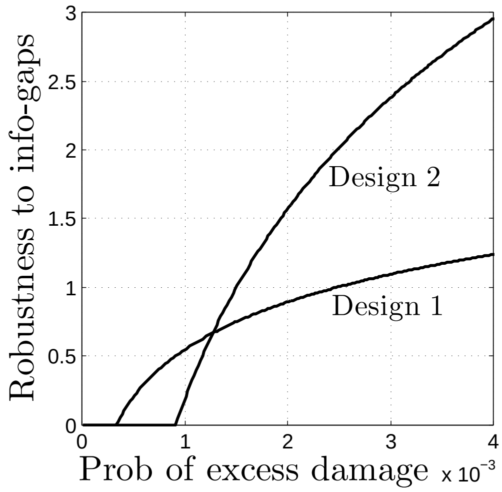
§ Outcome optimization:

- **Find best models. (Maybe probability.)**
- **Predict best-outcome design.**

§ Robust-satisficing:

- **Identify critical outcome.**
- **Maximize rbs of critical outcome.**

§ Optimize or robust-satisfice?

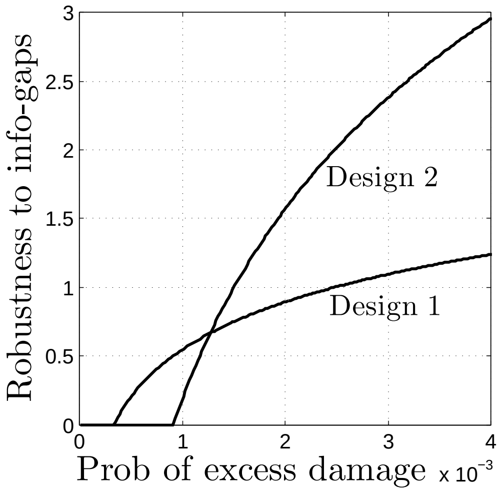


§ Outcome optimization:

Des 1 predicted better than Des 2.

§

§ Optimize or robust-satisfice?



§ Outcome optimization:

Des 1 predicted better than Des 2.

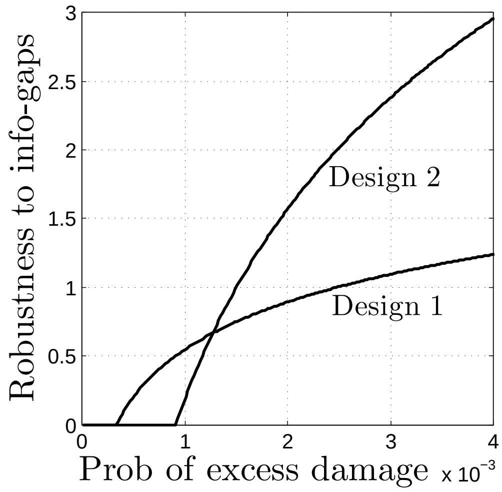
§ Predictions have zero robustness.

§ Robust-satisficing:

Design 2 more robust for $P > P_{\times}$.

§

§ Optimize or robust-satisfice?



§ Outcome optimization:

Des 1 predicted better than Des 2.

§ Predictions have zero robustness.

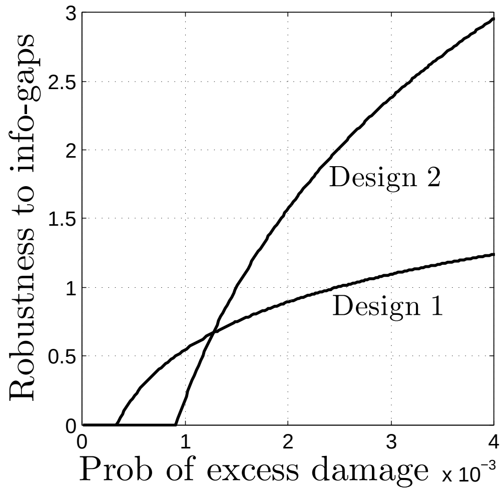
§ Robust-satisficing:

Design 2 more robust for $P > P_\times$.

§ Resolve innovation dilemma:

- **Value judgment on outcome requirement.**
- **Robustly satisfy requirement.**

§ Optimize or robust-satisfice?



§ Robust-satisficing strategy:

Robustly satisfy performance requirement.

§ Question:

Is robustness a good bet?

7 Conclusion

§ **Lessons:**

- **Design for no-failure.**
- **Prepare Disaster Recovery Capability.**

§

§ **Lessons:**

- **Design for no-failure.**
- **Prepare Disaster Recovery Capability.**

§ **Challenges:**

- **Why do we need DRC if we do No-Fail Design?**
  - **Resource allocation.**
  - **Public relations.**
-

§ **Lessons:**

- **Design for no-failure.**
- **Prepare Disaster Recovery Capability.**

§ **Challenges:**

- **Why do we need DRC if we do No-Fail Design?**
  - **Resource allocation.**
  - **Public relations.**
- **Moral hazard:**
  - **Design & DRC teams: cooperate.**
  - **Design & DRC teams: independent.**
-

§ **Lessons:**

- **Design for no-failure.**
- **Prepare Disaster Recovery Capability.**

§ **Challenges:**

- **Why do we need DRC if we do No-Fail Design?**
  - **Resource allocation.**
  - **Public relations.**
- **Moral hazard:**
  - **Design & DRC teams: cooperate.**
  - **Design & DRC teams: independent.**
- **Uncertainty:**
  - **Can we optimize?**
  - **Can we reliably predict performance?**

§

§ Lessons:

- Design for no-failure.
- Prepare Disaster Recovery Capability.

§ Challenges:

- Why do we need DRC if we do No-Fail Design?
  - Resource allocation.
  - Public relations.
- Moral hazard:
  - Design & DRC teams: cooperate.
  - Design & DRC teams: independent.
- Uncertainty:
  - Can we optimize?
  - Can we reliably predict performance?

§ Closing question:

No-fail design and disaster recovery capability are both necessary for critical technology.

How to decide the technology is feasible?